Deprecating Obsolete Key Exchange Methods in TLS

Nimrod Aviram
with moral support from Carrick Bartle and Chris Wood

TL;DR

- ❌ RSA Key Exchange
- 👍 FFDHE: Only in well-known group >= 2048 bit.
  - (Reminder: deprecate-ffdh already says only fully ephemeral FFDHE, no FFDH)

Is this practical? (YES!)

- Consistent with recommended configuration in Mozilla's Server Side TLS Guide (link)
- "compatible with nearly every client released in the last five [by now, six] years."

Reminder: RSA Key Exchange = Attack Surface

- No Forward Secrecy
- RSA cipher suites already not recommended.
- New Bleichenbacher Attack every few years (ROBOT, DROWN, Usenix 2014)
- No key separation: One server vulnerable to Bleichenbacher’s attack = all servers with same key vulnerable.
    - (also affects Delegated Credentials)

Reminder: The Woes of FFDHE

- No mechanism for negotiating the group size
- Current Discrete Log record: 795 bits
  - So 1024 bit FFDHE is insecure.
  - Discrete Log computation is expensive per group. Once done, cheap per exponent.
- If not fully ephemeral: Raccoon Attack.
- With weird groups: Subgroup Attacks.

TL;DR, again

- ❌ RSA Key Exchange
- 👍 FFDHE: Only in well-known group >= 2048 bit.
- Recommended by Mozilla, compatible with nearly every client released in the last six years.